A Multimodal Authorization Approach for Integrated Access Control Process

Shamma Alhameli, Noof Alhammadi and Richard Ikuesan
Computing and Applied Intelligence, College of Technological Innovation, Zayed University, Abu Dhabi, UAE

shammaalhameli21@gmail.com
nouffalham@gmail.com
richard.ikuesan@zu.ac.ae

Abstract: Traditional authorization mechanisms such as passwords, smart cards, and conventional biometrics remain vulnerable to spoofing, replay, and social-engineering attacks, particularly in IoT and cloud environments. Physiological biometrics, including electrocardiogram (ECG) and electromyography (EMG) signals, offer stronger resistance to forgery because of their biological origin while also capturing emotional and behavioral context. This study presents AlMuwathiq, an emotion-based multimodal authorization system that integrates ECG and EMG signals to support adaptive access-control decisions. Real physiological signals were collected and labeled using the Self-Assessment Manikin across five emotional states. After signal preprocessing and feature extraction, multiple machine learning models were evaluated, with a focus on explainable learning algorithms. Experimental results indicate that Random Forest and XGBoost achieved the most stable classification performance. The trained models were integrated into a real-time platform where access control authorization decisions are determined by emotional rules. The findings demonstrate that emotion-aware physiological authorization can enhance security, reliability, and context awareness in modern cybersecurity systems. This study thus advances the current state of the art in access control systems, especially in mission-critical infrastructures.

Keywords: Emotion-based authorization, Physiological biometrics, Electrocardiogram (ECG), Electromyography (EMG), Multimodal authentication, Affective computing, Machine learning, Access control, Cybersecurity

1. Introduction

Authentication is a fundamental security mechanism that verifies users' identities and grants access only to authorized individuals. It plays a critical role in protecting systems and sensitive data from unauthorized access. This process typically relies on three main factors: something the user knows (such as passwords), something the user has (such as tokens or smart cards), and something the user is (biometric characteristics). While these methods are widely used due to their simplicity and ease of implementation, they also suffer from several limitations. Password-based authentication, for example, is highly vulnerable to brute-force attacks, phishing, and credential theft (Florêncio & Herley, 2007). Similarly, token-based methods may fail if the physical device is lost, stolen, or duplicated, which creates additional security risks. There are many authentication challenges in the Internet of Things (IoT), including security risks that might threaten network security. Examples include man-in-the-middle attacks, in which an attacker sits between two parties and intercepts data as it is transferred, and brute-force attacks, which repeatedly guess passwords. In addition, there are privacy concerns; biometric data such as iris scans, fingerprints, and voice recognition can be collected, and the user's location can be saved with the data. This can lead to unauthorized tracking, which is a major privacy issue. Moreover, there is a concern about flexibility, as many devices require authentication to maintain a high level of security and support intelligent solutions such as artificial intelligence. Resource limitations are another challenge, since devices often have limited memory and battery power (Alsheavi et al., 2024).

A typical user authentication process follows a structured sequence: an identity claim, credential submission, and verification against stored data (Adeyemi & Ithnin, 2012). If the credentials match, access is granted; otherwise, it is denied. However, traditional systems often rely on single-factor authentication, which significantly increases the risk of unauthorized access. Modern systems have therefore shifted toward multi-factor authentication (MFA), combining multiple verification methods to improve security. Despite these improvements, authentication alone is not sufficient. Authorization plays an equally important role, as it determines what actions a verified user is allowed to perform within a system. Authorization ensures that users only access resources that match their permission level. As highlighted in the project, authorization mechanisms follow specific rules that define access based on factors such as roles, policies, and system conditions. Common models include Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Policy-Based Access Control (PBAC). However, traditional authorization methods are often static and do not adapt to real-time conditions. In modern environments such as IoT and cloud systems, this creates serious challenges. Devices in these environments are often resource-constrained and may lack proper security configurations, making it difficult to enforce consistent access control policies (Khan et al., 2022). As a result, even if authentication is successful, weak authorization can still lead to security breaches. To address these limitations, researchers have explored more advanced profiling-based mechanisms that extend beyond static authentication and focus on continuously understanding user behavior and characteristics. These profiling approaches include multiple dimensions. User profiling enables adaptive systems to learn preferences over time through explicit and implicit data collection, thereby improving personalization and decision-making accuracy. Physiological profiling uses biological signals such as EEG, ECG, and GSR to measure cognitive states, such as attention and engagement, enabling systems to detect deeper user conditions. Sociological profiling examines how social structures and behavioral mechanisms influence human actions, highlighting ethical concerns when human behavior is oversimplified into machine-like processes. Linguistic profiling treats speech and writing patterns as a digital fingerprint by analyzing vocabulary, tone, and typing behavior for identity verification. Psychological profiling focuses on personality traits, such as the Big Five model, and is often applied to machine learning systems to infer behavioral tendencies, though it raises concerns about bias and fairness. Behavioral profiling enables continuous authentication through patterns such as typing, touch gestures, movement, and eye behavior, making identity verification ongoing rather than one-time. Together, these profiling mechanisms create a more adaptive and multi-dimensional understanding of users, but they also introduce challenges related to privacy, ethics, and data interpretation.

Building on these advancements, researchers have explored biometric-based approaches, particularly physiological biometrics. Unlike traditional biometrics such as fingerprints or facial recognition, physiological signals originate from within the human body, making them more secure and difficult to replicate. Two important physiological signals are the electrocardiogram (ECG) and electromyography (EMG). ECG signals measure the electrical activity of the heart, producing waveform patterns that are unique to each individual. EMG signals, on the other hand, measure muscle activity and reflect how muscles respond during movement or expression. As stated in the project, these signals "are difficult to forge and contain individual-specific patterns," making them highly suitable for authentication and authorization systems (Israel et al., 2005; Jain et al., 2016). In addition to identity verification, physiological signals provide valuable insights into a user's emotional state. This concept is supported by research in affective computing, which focuses on detecting and interpreting human emotions using computational methods. According to the project, physiological signals such as ECG and EMG can reflect emotional states like calmness, stress, and frustration, which may influence user behavior during access attempts. For example, a sudden increase in heart rate or muscle tension may indicate stress or abnormal conditions. Incorporating this emotional information into authorization decisions allows systems to become more context-aware and adaptive (Picard, 1997). Several studies have explored the relationship between ECG signals and emotional states. ECG-based emotion recognition typically analyzes features such as heart rate variability, waveform morphology, and frequency-domain characteristics. Similarly, EMG signals—especially those collected from facial muscles—can be used to detect emotions such as happiness, anger, and sadness by analyzing muscle activation patterns. Machine learning techniques play a crucial role in this process. Algorithms such as Support Vector Machines (SVMs), Random Forests, K-Nearest Neighbors (KNNs), and deep learning models are commonly used to classify emotional states based on extracted features. These models learn patterns from labeled datasets and can achieve high accuracy in recognizing different emotions. To further improve system performance, researchers have introduced multimodal biometric systems that combine multiple physiological signals. Instead of relying on a single signal, multimodal systems integrate ECG and EMG data to enhance accuracy and reliability. As mentioned in the project, combining multiple signals helps "reduce noise, improve classification performance, and increase resistance to spoofing attacks". This approach is particularly useful in real-world scenarios where signal quality may vary due to movement or environmental conditions. Multimodal systems also provide better robustness, as they rely on multiple sources of information rather than a single point of failure (Ross & Jain, 2004).

Despite the advantages of physiological biometric systems, several limitations still exist in current research. Many existing studies focus on ECG or EMG signals independently, without fully exploring the benefits of combining the two modalities in a unified framework. In addition, most traditional systems rely primarily on identity verification and do not consider the user's emotional or behavioral context during access attempts. This creates a gap where authorized users may still gain access under abnormal or high-risk conditions, such as stress or coercion. Furthermore, challenges such as signal variability, noise interference, and privacy concerns continue to affect the reliability and real-world applicability of these systems. While preprocessing and machine learning techniques have improved classification performance, there is still a need for systems that can operate reliably in dynamic environments while maintaining user privacy and security (Khan et al., 2020; Meltzer & Luengo, 2023; Wang et al., 2025). Therefore, this study builds on existing research by proposing a multimodal authorization approach that integrates both ECG and EMG signals with emotional state recognition. By combining multiple physiological signals and incorporating emotional awareness into access control decisions, the proposed system aims to provide a more secure, adaptive, and context-aware authorization mechanism compared to traditional methods.

2. Background of the Study

This section reviews existing studies related to electrocardiogram (ECG) and electromyogram (EMG) biosignal technologies, with a focus on privacy, authorization mechanisms, and data security challenges. It examines identified risks, such as unauthorized access and re-identification, and emphasizes the need for structured authorization and forensic-aware frameworks to support the secure and ethical management of biosignal data within wearable and remote healthcare systems. With the rapid growth of wearable and remote healthcare technologies, the privacy and authorization of biosignals such as electrocardiogram (ECG) and electromyogram (EMG) data have become increasingly critical research concerns. These signals are widely used in clinical environments and biomedical research for their diagnostic value; however, their high sensitivity raises serious concerns about data access, misuse, and patient privacy. Prior studies have shown that ECG data, in particular, can reveal uniquely identifiable and personal information. Wang et al. (2025) demonstrated that ECG datasets shared without proper anonymization are vulnerable to re-identification attacks, emphasizing the need for strict authorization mechanisms and controlled access. Similarly, Meltzer and Luengo (2023) highlighted that the intrinsic uniqueness of ECG signals makes them comparable to biometric identifiers, meaning that even short recordings can expose sensitive health-related details if accessed without appropriate safeguards.

From a legal and ethical perspective, healthcare regulations such as the Health Insurance Portability and Accountability Act (HIPAA) mandate explicit patient authorization before biosignal data can be accessed or shared. These regulatory frameworks emphasize accountability and informed consent, particularly when ECG and EMG data are collected, processed, or transmitted through online and wearable systems. Overall, the literature consistently underscores the importance of robust authorization and privacy controls for the ethical, secure, and lawful management of biosignal data, especially as wearable medical devices become increasingly integrated into modern healthcare infrastructures. Although the advantages of ECG and EMG are based on systems, there are multiple challenges from different perspectives. From a security perspective, wearable and IoT environments can be vulnerable to unauthorized access and inadequate protection, putting sensitive data at high risk. From a technical side, these signals can be affected by noise, sensor placement, and changes in the user's condition, which may reduce accuracy. In addition, traditional authorization methods have limitations, such as the risk of stolen access cards or granting users more permissions than needed. To address these issues, our system (AlMuwathiq) uses a combination of ECG and EMG signals to create a more secure and reliable approach. It improves accuracy through signal processing and machine learning, and it makes smarter authorization decisions by also considering the user's emotional state, making the system more adaptive and secure.

3. Methodology

The methodology followed in this study is illustrated in the operational framework shown in Figure 1. The framework consists of a setup phase and three main phases covering dataset development, signal preprocessing, machine learning experimentation, and the final integration of the authorization platform. Each stage reflects the actual workflow used to implement the access control system (hereinafter, the AlMuwathiq system).

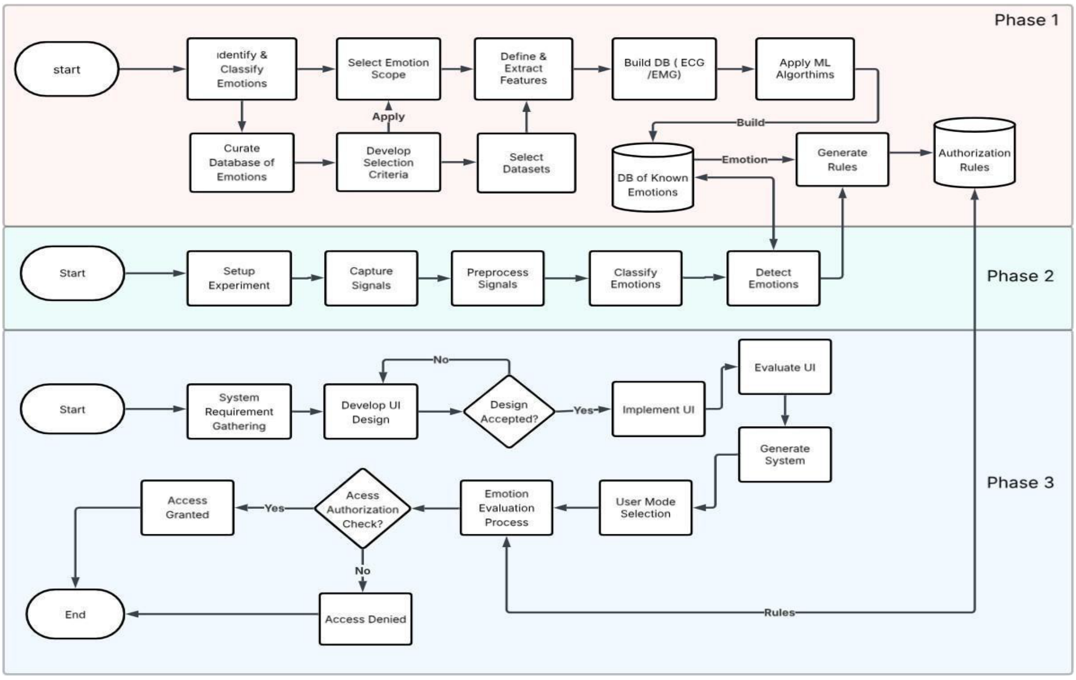

Figure 1: Operational Framework

3.1 Setup Phase

In the setup phase, the ECG and EMG sensors were carefully connected to the hardware device and allowed to ensure reliable signal acquisition. The Arduino was configured to read the analog inputs from both sensors and transmit the recorded values for further processing. The software environment, including Python and required packages, was prepared to support the preprocessing, feature extraction, and machine learning stages of the study. Table 1 provides an overview of all components used in the system configuration.

Table 1: Tools, Sensors, and Software Used in the System

Component	Description
ECG Sensor	Captures electrical heart activity through analog pin A0
EMG Sensor	Measures muscle activation through analog pins A1 and A3
Arduino Board	Acquires raw signals and transmits them via serial output
Python	Used for preprocessing and machine learning
Platform	Allows users to upload signals and receive authorization results

3.2 Phase I: Dataset Development

In this phase, real ECG and EMG signals were collected from users using the configured hardware device. Signals were captured in real time and exported as CSV files. Each recording was labeled with one of the five emotional categories defined in the system: Calm, Amused, Satisfied, Gloomy, or Frustrated. To ensure labeling is correct, the Self-Assessment Manikin (SAM) was administered after each recording. The SAM values were used as ground-truth labels for the machine-learning dataset (Handayani et al., 2015).

3.3 Phase II: Signal Preprocessing and Feature Extraction

Raw ECG and EMG signals contain noise and irregularities; therefore, a preprocessing pipeline was implemented. Signal cleaning included:

- Bandpass filtering to isolate relevant frequency ranges

- Notch filtering to remove 50/60 Hz power-line noise
- Smoothing and denoising to reduce signal artifacts
- Windowing by dividing the signal into equal segments

After preprocessing, features were extracted from each window. The features listed below match the actual feature sets used

Table 2: ECG Feature Set Extracted

Feature Category	Extracted Features
Time-Domain	Mean, Standard Deviation (STD), Root Mean Square (RMS), Peak-to-Peak
Frequency-Domain	Power Spectral Density (PSD-based features), Dominant Frequency
Statistical Features	Variance, Skewness, Kurtosis
Morphological	R-peak information (from processed ECG waveform when applicable)

Table 3: EMG Feature Set Extracted

Feature Category	Extracted Features
Time-Domain	Mean Absolute Value (MAV), Root Mean Square (RMS), Waveform Length (WL)
Frequency-Domain	Median Frequency, Mean Frequency
Statistical	Variance, Log Energy Entropy
Signal Shape Features	Slope Sign Changes (SSC), Zero Crossings (ZC)

3.4 Phase III: Machine Learning Experimentation

The extracted features were used to train and evaluate multiple classification models. The algorithms tested include:

- Random Forest
- XGBoost
- Support Vector Machine (SVM)
- K-Nearest Neighbors (KNN)

Model performance was evaluated using accuracy, precision, recall, F1-score, and confusion matrix. Two experiments were carried out: an initial experiment and an optimized version after refining the preprocessing pipeline and dataset structure. The following table summarizes the general performance patterns of the models based on your results.

Table 4: Model Evaluation Overview

Model	Performance Summary
Random Forest	Strong and stable performance; among the highest accuracy and F1-score in both experiments
XGBoost	High accuracy and strong performance after optimization
SVM	Moderate performance; sensitive to noise and variability
KNN	Lowest performance; not suitable for this dataset

3.5 Authorization System Development

In this final phase, the trained models were integrated into the AlMuwathiq authorization platform. The system allows users to upload an ECG or EMG CSV file, select a classification model, and receive an emotion prediction, after which access is automatically granted or denied based on predefined emotional rules.

Emotional authorization rules used:

- Calm, Satisfied, Amused → Access Granted
- Gloomy, Frustrated → Access Denied

4. Discussion

The results of this project demonstrate that integrating privacy-aware authorization mechanisms into biosignal-based systems is both necessary and feasible. The findings confirm that ECG and EMG signals are not only valuable for health monitoring and authentication, but also pose significant privacy risks when handled without strict access controls. Throughout the project, the implemented authorization approach showed that limiting access based on predefined conditions and user roles can effectively reduce the exposure of sensitive biosignal data. This supports the argument presented in the literature that biosignals should not be treated as ordinary medical data, but rather as high-risk biometric-like information requiring stronger protection.

From a system perspective, the final project successfully translates theoretical privacy and authorization concerns into a practical framework. The results indicate that combining authorization logic with biosignal processing enhances data security without disrupting system functionality or usability. This balance is critical in wearable and remote healthcare environments, where continuous data collection is required. Moreover, the project highlights that simple anonymization alone is insufficient, as ECG characteristics remain identifiable even in limited samples. By enforcing controlled access and explicit authorization, the system aligns more closely with legal and ethical requirements such as patient consent and accountability, as emphasized by healthcare regulations.

Overall, the project outcomes validate the proposed approach and demonstrate its relevance to real-world applications involving wearable medical devices. The results contribute to existing research by showing how authorization mechanisms can be practically embedded within biosignal systems rather than treated as an external policy layer. While the project is limited to a controlled experimental setup, it establishes a strong foundation for future work, including real-time deployment, larger datasets, and integration with advanced security frameworks. In conclusion, the results confirm that privacy-preserving authorization is a critical component for the secure and ethical use of ECG and EMG technologies, reinforcing the overall objectives of the final project.

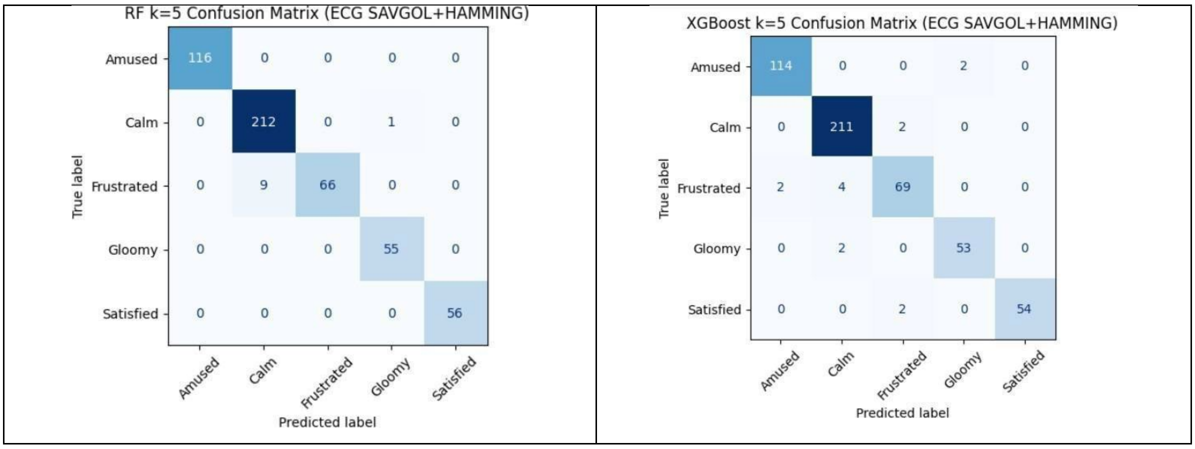

Figure 2-3: Confusion Matrix for Random Forest & XGBoost (k=5) using ECG SAVGOL+HAMMING

The confusion matrix analyses provide strong evidence of the effectiveness and stability of the proposed multimodal emotion-based authorization framework. Across both ECG and EMG modalities, the evaluated models demonstrate a dominant diagonal structure, indicating that the majority of samples were correctly classified into their respective emotional categories. In particular, the ECG-based results using the SAVGOL+HAMMING preprocessing configuration show consistently high recognition performance for all five emotional states. The limited misclassifications observed—primarily between Frustrated and Calm—suggest that these emotions share partially overlapping physiological characteristics, a phenomenon commonly reported in affective computing literature. Nevertheless, the overall classification stability indicates that the selected ECG preprocessing pipeline preserves discriminative emotional features while remaining robust.

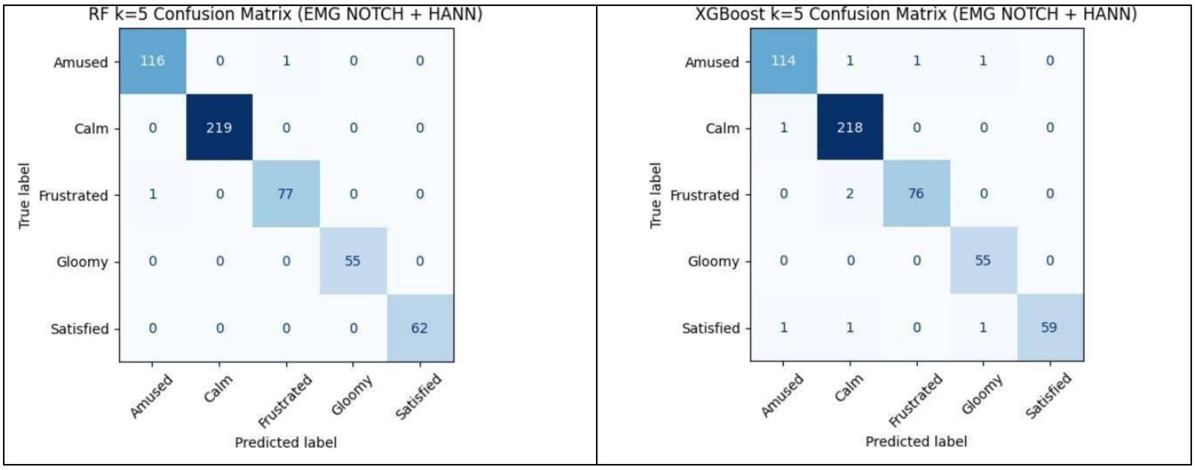

Figure 4-5: Confusion Matrix for Random Forest & XGBoost (k=5) using EMG NOTCH+HANN

A similar trend is observed for EMG-based emotion recognition, where the NOTCH+HANN preprocessing configuration yields highly reliable results. The Random Forest classifier exhibits near-perfect diagonal dominance, with only two isolated misclassifications, indicating exceptional consistency and generalization capability. While the XGBoost model also achieves strong performance, it displays slightly increased confusion among certain emotional classes, particularly Amused and Satisfied. This difference highlights the comparative stability of Random Forest in handling EMG signal variability and noise, reinforcing its suitability for biosignal-driven authorization tasks. Overall, the results suggest that EMG signals, when appropriately filtered and windowed, can offer highly distinctive emotional patterns that support secure and accurate classification.

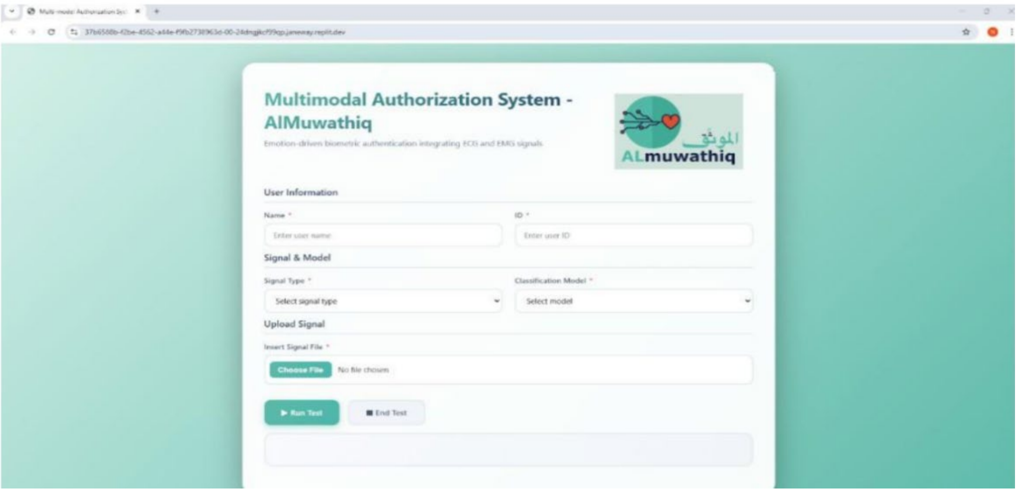

Figure 6: User Interface of the AlMuwathiq Multimodal Authorization System

Beyond model performance, these results directly validate the design and functionality of the AlMuwathiq Multimodal Authorization System. The system successfully translates emotion classification outputs into real-time authorization decisions through a clear rule-based mechanism. The user interface results demonstrate that detected emotions are transparently mapped to access outcomes, ensuring both usability and explainability—key requirements for authorization systems in sensitive environments. The correct handling of both access-granted and access-denied scenarios confirms that the system operates as intended, enforcing emotional-state-based authorization without ambiguity. Taken together, the results confirm that the proposed framework is not only technically sound but also practically deployable, offering a secure, interpretable, and privacy-aware approach to biosignal-based authorization suitable for real-world applications. In summary, this methodology outlines the complete scientific workflow of the AlMuwathiq system: real signal acquisition, SAM-based emotional labeling, structured preprocessing, feature extraction, machine learning experimentation, and final system deployment. All steps described directly reflect the project implementation without adding any external methods or assumptions.

5. Future Studies and Recommendations

Future work on the proposed AlMuwathiq system will focus on expanding the dataset and improving the stability of emotion classification across a wider range of users. Since the current dataset was collected from a limited group, increasing the number of participants would strengthen the reliability and generalization of the emotional categories. Additional data samples would also support further refinement of the preprocessing pipeline, particularly in reducing naturally occurring noise in ECG and EMG recordings. In addition, enhancing the performance of the existing machine-learning models. While Random Forest and XGBoost demonstrated strong results in the evaluation, further optimization of the feature sets and preprocessing techniques may lead to even more consistent outcomes. This can include refining windowing strategies or exploring additional parameters within the current feature categories already used in the project. Moreover, future versions of the system could focus on improving the user experience of the authorization platform. This includes streamlining the signal upload process, improving the visualization of emotional output, and ensuring the authorization decision is clearly communicated to the end user. Integrating additional testing scenarios within the platform may also help validate the system's behavior in different usage conditions. Finally, future studies should examine how the emotional states captured by ECG and EMG signals evolve across multiple sessions and different time periods. This will help maintain long-term consistency in emotional biometrics and evaluate whether the same emotional patterns remain stable across repeated use. Such insights would help improve the system's reliability and position emotion-based authorization as a viable complement to traditional authentication methods.

6. Conclusion

The concept of user and entity authorization has been widely deployed for access control in mission-critical infrastructure. Existing studies have shown the need for a dynamic mechanism that considers the user's emotional and psychological state before authorization. This study developed an innovative mechanism for entity authorization that considers the user's emotional state using a widely accepted emotion classification metric. The results of a comprehensive experimental and testing process further validate the study's proposition and establish a reliable accuracy threshold. The results of this study, therefore, demonstrate that both ECG and EMG signals from users can be leveraged for authorization. Furthermore, this probability opens the possibility of integrating emotion-based authorization as a complementary component in physical security.

Ethics Declaration: This study did not require ethical approval because no human or animal subjects were involved. The authors affirm that no human research participants were involved in this study; hence, it is not applicable.

AI Declaration: The Authors declare that AI was not used to write the manuscript and that the content represents the authors' original writing, except where an AI tool was used to edit the manuscript to enhance clarity.

References

Adeyemi, I. R., & Ithnin, N. B. (2012). Bio-Thentic Card: Authentication concept for RFID Card. *arXiv preprint arXiv:1210.5913*.

Alsheavi et al.,Computing Surveys, 2024, doi: 10.1145/3703444."IoT authentication protocols: Challenges, and comparative analysis," ACM

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International World Wide Web Conference (WWW)*, 657–666. https://doi.org/10.1145/1242572.1242661

Handayani, D., Wahab, A., & Yaacob, H. (2015). Recognition of emotions in video clips: The Self-Assessment Manikin validation. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *13*(4), 1343–1350. https://telkomnika.uad.ac.id/index.php/TELKOMNIKA/article/view/2735/1891

Israel, S. A., Irvine, J. M., Cheng, A., Wiederhold, M. D., & Wiederhold, B. K. (2005). ECG to identify individuals. *Pattern Recognition*, *38*(1), 133–142. https://doi.org/10.1016/j.patcog.2004.05.014

Jain, A. K., Ross, A., & Nandakumar, K. (2016). *Introduction to biometrics*. Springer. https://doi.org/10.1007/978-0-387-77326-1

Khan, M. A., Salah, K., Jayaraman, R., & Arshad, J. (2020). Trust-based access control for IoT-based smart environments. *Future Generation Computer Systems*, *108*, 653–665. https://doi.org/10.1016/j.future.2020.03.030

Khan, M. A., Alzahrani, B. A., & Salah, K. (2022). Authorization and access control challenges in IoT environments. *IEEE Access*, *10*, 22561–22574. https://doi.org/10.1109/ACCESS.2022.3154952

Meltzer, J., & Luengo, D. (2023). ECG-based biometric recognition: Security and privacy challenges. *Sensors*, *25*(6), Article 1864. https://www.mdpi.com/1424-8220/25/6/1864

Picard, R. W. (1997). *Affective computing*. MIT Press. https://mitpress.mit.edu/9780262661154/affective-computing/

Ross, A., & Jain, A. K. (2004). Multimodal biometrics: An overview. *Proceedings of the 12th European Signal Processing Conference (EUSIPCO)*, 1221–1224.

Wang, Y., et al. (2025). ECG privacy risks and re-identification attacks. *arXiv*. https://arxiv.org/abs/2508.15850